JENNIFER M. GRANHOLM
GOVERNOR

STATE OF MICHIGAN
OFFICE OF FINANCIAL AND INSURANCE SERVICES
DEPARTMENT OF CONSUMER & INDUSTRY SERVICES
DAVID C. HOLLISTER, DIRECTOR

LINDA A. WATTERS
COMMISSIONER

DATE: June 23, 2005

LETTER NO.: 2005-CU-09

TO: The Board of Directors and Management of Michigan State-Chartered Credit Unions

SUBJECT: Internet Financial Services

This letter replaces Letter 2000-CU-01.

The purpose of this letter is to advise credit union officials of important considerations when entering into, using, or providing internet financial services. The internet is inherently insecure and Officials should be knowledgeable of potential threats. Internet financial services present greater risk than in-house or serviced environments. If vendor services are used, controls may also be more difficult to monitor.

Officials must consider the following internet financial services issues. The Office of Financial and Insurance Services (OFIS) will review these areas during our regulatory examinations.

Planning and Due Diligence

Officials must thoroughly consider all internet financial services aspects that affect the credit union. Identification and comprehension of applicable risks, establishment of appropriate controls, determination of costs and benefits on the strategic plan, and development of an ongoing monitoring program is essential. Officials must analyze links to other third party services (through portal-type connections) to understand the network arrangement, controls, and security implications. This due diligence must be documented.

Risks and Controls

Risk identification and control is important. Risks may arise from internal and external sources. Officials must assess the degree of risk exposure and adopt controls to mitigate potential threats to the credit union and its members. Risks are ever evolving and the identification is often imperfect. Accordingly, Officials must review risks and internal controls on an ongoing basis. Internal and external audit functions must include a review of internet financial services and controls.

Vendor Reliance

Officials are ultimately responsible for the business affairs, funds, and records of the credit union. Many credit union officials, however, place significant reliance on third party service providers for security, data integrity, performance monitoring, and controls. To validate appropriate controls are in place, management must obtain documentation of the network

configurations, monitor service provider's performance, test service providers' backup - dependent functions, employ intrusion detection with immediate notification and/or disabling of the system, and analyze the service provider's financial viability through audited financial statements.

Officials must enter into a written contract, lease, or licensing agreement for third party providers' services, as required by Section 408 of the Michigan Credit Union Act. The Board of Directors must approve the contract, lease, or licensing agreement, and legal counsel should review the documents to protect the interests of the credit union.

Insurance
Officials must obtain adequate insurance coverage to cover potential liabilities relating to internet financial services, including specific coverage of "electronic crime" and, if applicable, vendor liability and employee bonding.

Disclosures
Officials must inform members of the risks associated with use of internet financial services. Disclosures must be accurate and comply with regulatory requirements. Informational web pages must also contain complete and accurate disclosures.

Privacy
Compromise of financial transactions or member information could result in regulatory and/or legal action, adversely impacting the credit union's reputation. Protection of member information is paramount to continued trusted service. Management should frequently review privacy laws and internal controls to comply.

Password Administration
Password administration is an area of concern for all computer services, not just those provided through the internet. Passwords should be at least a combination of eight alpha, numerical, case-sensitive, or special characters. Passwords should be known only by the owner, changed quarterly, and difficult to guess. If initial password are assigned, the password must not be the member's audio pin number, and should require a forced password change by the member before the accounts can be further accessed.

Conclusion
Involvement in internet financial services pose significant risks to credit unions. Accordingly, officials must consider the above issues while entering and engaging in internet financial services. The following website provides useful information on internet financial services:

www.ncua.gov
www.ffiec.gov
www.fdic.gov/regulations/index.html

www.ny.frb.org/bankinfo/circular/outsource.pdf
www.ots.treas.gov/ebanking.html

If you have any questions concerning this letter or other issues related to internet financial services, please contact our office.

Sincerely,

Roger W. Little, Deputy Commissioner
Credit Union Division